DRN-3797408

The complaint

Mrs D complains that Starling Bank Limited ('Starling') debited her account with a series of payments totalling approximately 2850 euros and £1000, which she says she did not make or otherwise authorise.

What happened

In March 2022, Mrs D was in hospital in another country for a medical procedure. When she was going back in for a follow up appointment, she explained she looked at her Starling app through her tablet and noticed transactions which she says she did not make or otherwise authorise. These are as follows:

- Three card payments to merchants, one of which was reversed by Starling. The payments which went through totaling approximately 2850 euros;
- Transfers between her foreign currency account and her GBP account; and
- A £1,000 card payment to a cryptocurrency company (which she noticed later when she reported the matter to the police). This was authenticated through the Starling app. Prior to this payment, another payment was attempted but declined due to insufficient funds. Money was then moved from the foreign currency account to fund this payment to cryptocurrency.

These payments were all made on the same day, within a span of roughly ten minutes. Mrs D did not notice them immediately as she said she had not looked at her Starling account. Once she saw them, she explained that she got in touch with Starling to tell them that she had not made these payments.

In further support of her position that she had not made or otherwise authorised these transactions, Mrs D said, in summary, that:

- the payments were not in line with how she usually made payments – she normally made small payments and used her physical card;
- she had contacted the retailer when she thought the payments were still pending, in the hope they could be stopped;
- she had been asleep and had not approved any notifications through the Starling app;
- she had never made a payment to cryptocurrency before and could not find out about the cryptocurrency account as it was not in her name;
- she reported the matter to the police in the country she was in;
- the only other person who could get into her phone or tablet was her husband, and he had not made or authorised these payments either;
- she was not familiar with the merchants the money went to, and having looked into them she thought they were the same company;
- her and her husband had no need to make any fraudulent transactions, and thought that this had to be an elaborate fraud;

- Mrs D provided an email from the retailer which said that they hadn't received orders from someone in her name at the specified dates and times (though it is not visible which dates and times were specified).
- her phone was not working and was off, in a drawer at home, when the disputed transactions took place.

Starling looked into what happened and declined to refund the disputed transactions. In summary, they thought it was most likely that Mrs D authorised the transactions. They said they would not refund the disputed transactions because:

- that payments were authorised using the app on one of Mrs D's registered devices which would have required either biometrics or the passcode, as well as the password to get into the phone or tablet;
- Mrs D was the only person with access to the registered device and app, so they did not see how someone else could have completed the payments without her involvement.

Unhappy with Starling's response, Mrs D brought her complaint to our service. One of our investigators looked into what had happened and did not recommend that the complaint be upheld. This was because they thought it was more likely than not that Mrs D made or otherwise authorised the disputed transactions, and so they did not think it would be fair and reasonable to ask Starling to refund them.

Mrs D remained dissatisfied. Amongst other points in line with those referenced earlier in this decision, she said:

- the fact that Starling refused to say how the payments had been biometrically authorised showed that the account must have been hacked and questioned why this option had not been investigated;
- that she could tell us the IP address of her device, and it would surely not match that present for the disputed transactions;
- our investigator had been incorrect when they said only one device was registered with the Starling app, as she had her phone and tablet registered.

Our investigator's opinion was not changed, so the case was passed to me to decide.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I have reached the same conclusion as our investigator, and broadly for the same reasons. I know this will come as a disappointment to Mrs D, particularly as she has been waiting for a long time for an answer, and I am sorry for this. I will explain how I have reached this conclusion.

Generally, Starling can hold Mrs D liable for the disputed transactions if the evidence suggests that it is more likely than not that she authorised these payments or gave someone else consent to make them on their behalf. I'm satisfied from my review of Starling's technical evidence that the payments were properly authenticated firstly by the correct details being given to the merchants which for card payments would include the long card number and correct personal details. I am also satisfied from Starling's technical evidence that further to this, someone had to authenticate the payments using the Starling app. This means that when the payments were attempted, an alert was sent to a device with Mrs D's registered Starling app on it, and someone confirmed that the payment was genuine. I am

not clear from the evidence provided whether biometrics or a passcode were used to open the Starling app, but one would have been required. So, I am satisfied that the payments were properly authenticated. But the regulations relevant to this case say that is not, on its own, enough to enable Starling to hold Mrs D liable. So, I need to think about whether the evidence suggests that it is more likely than not that Mrs D consented to these transactions being made, which could include allowing someone else to complete these transactions on her behalf. Having done so, on balance, I think that Mrs D must have made or otherwise authorised these transactions. I say this because:

- The technical evidence shows that the transactions took place on one of Mrs D's registered devices. Mrs D is correct that there were two devices registered with her Starling app – a tablet and a mobile phone. Mrs D has explained that her phone was not working and in a drawer at home. I've thought about whether the phone not working could have been an indication that it had been infected with some kind of malware, or whether the device could have otherwise been taken over. On balance I don't think this is likely what happened. I say this because Mrs D explained the phone was off and uncharged, and even if an unknown third party had got into this device by technical and malicious means, I've not been able to find evidence that suggests it is likely that transactions can take place on a device which is not switched on. So, I think it is most likely that the transactions took place on Mrs D's tablet.
- By Mrs D's own admission, she had her tablet with her and the only people who could have accessed it were her and her husband. Someone needed to get into the tablet, and the Starling app in order to authenticate the payments. And it seems unlikely that an unknown third party was able to get access to her tablet, then get into the tablet and the Starling app without her knowledge.
- The person making the payments also needed to know the details of Mrs D's card. Mrs D has explained that she had this with her and used it for genuine transactions around this time. It seems unlikely that an unknown third party would have been able to get the card details from her physical card without her noticing – as the same person would have had to have access to her tablet. Card details can also be viewed within the Starling app, but as I explained above I cannot see how an unknown third party could have got into Mrs D's app so I cannot see how someone would have accessed her card details this way.
- The IP address that was used to access Mrs D's starling app was consistent before, during and after the disputed transactions took place. Whilst this is not conclusive evidence, it does suggest that the tablet was connected to the internet in the same way throughout this period.

So, on balance I think it is most likely that Mrs D authorised these payments or allowed someone else to do so on her behalf.

I've thought about whether Starling ought to have intervened with any of these payments. In some circumstances, in accordance with the relevant regulations, rules and best practice from the time the payments were made, I would expect Starling to intervene and ask more questions about payments which were unusual or out of character for a customer. There is a delicate balance to strike between this, and their overriding obligation to process payments in a timely manner. So, whilst the payments were not for insignificant amounts, I don't think they were sufficiently unusual and out of character that they ought to have intervened here. I accept Mrs D's point that she has never purchased cryptocurrency before, but I don't think that this meant that Starling ought to have intervened with the payment. These payments were larger in value than Mrs D's normal payments, but not so large that I think they demonstrated a clear risk that Mrs D was falling victim to fraud or financial crime. So, I don't think Starling acted incorrectly in following the payment instructions here.

I am sorry as I know this will come as a disappointment to Mrs D. I have thought for a long time about this case, as I do believe that there is a possibility of third-party involvement in some way in these funds going to cryptocurrency and to the retailers in question. Mrs D has been consistent in her testimony that she did not and would not make payments to these companies - and I do think whilst the spending was not so unusual that Starling ought to have intervened, it was unusual for Mrs D. Mrs D has not indicated that she was tricked or coerced into making these payments, but I cannot rule out that this is the case. But, with the evidence available to me I cannot find a plausible way that an unknown third party could have made these payments, and so on the question of whether they can be considered authorised by Mrs D or someone acting with her consent – the evidence leads me to conclude that they were. And so it follows that Starling acted correctly in declining the refund.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs D to accept or reject my decision before 28 February 2025.

Katherine Jones
Ombudsman